UNITED STATES DISTRICT COURT

for the

District of South Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Silver Apple iPhone "S" Model A1688 cellular phone

Case No. 2:22-cr-201

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of South Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(o)	Knowing possession of a machinegun
18 U.S.C. 922(g)(1)	Felon in possession of a firearm/ammunition
21 U.S.C. 841(a)(1)	Possession with intent to distribute a controlled substance

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ROBERT CALLAHAN Digitally signed by ROBERT CALLAHAN Date: 2022.02.02 09:18:47 -05'00'

Applicant's signature

Robert E. Callahan, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: 02/02/2022

Mary Gordon Baker

Judge's signature

City and state: Charleston, South Carolina

Mary Gordon Baker, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
BEAUFORT DIVISION

IN THE MATTER OF THE SEARCH OF A MOTOROLA TYPE: N57C9, IPHONE "S" MODEL A1688 AND AN IPHONE (PRODUCT) RED	Case No. 2:22-cr-201

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Robert Callahan, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – digital devices – which are currently in law enforcement possession (the "Devices"), as described in attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Department of Justice. I have been so employed by ATF since 2009. I have a Bachelor of Science degree in Criminal Justice received from the University of South Carolina. I am a graduate of the Criminal Investigator Training Program from the Federal Law Enforcement Training Center as well as a graduate of Special Agent Basic Training from the ATF National Academy. I am currently assigned to the ATF Charleston Field Office within the Charlotte Field Division. My primary duties include investigating violations of the federal firearms laws, gang activity, and violent crime. I have participated in investigations involving state and federal firearm violations, illegal firearms trafficking, illegal narcotics trafficking,

armed drug trafficking, racketeering violations, criminal enterprises and criminal street gangs. Accordingly, I am thoroughly familiar with the investigative techniques used in these investigations, such as the use of undercover agents, the use of cooperating witnesses and confidential informants, surveillance, search and seizure warrants, and the extraction and analysis of data from cellular telephones. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 922(o), 18 U.S.C. § 922(g)(1), 18 U.S.C. § 924(c), 21 U.S.C. § 841(a)(1), 26 U.S.C. § 5861(d), and 26 U.S.C. § 5861(e) have been committed by Tyrone Evan Lewis GRAYSON. There is also probable cause to search the Devices, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is further described as a Motorola Type: N57C9 cellular phone (blue in color), Apple iPhone "S" Model A1688 cellular phone, (silver in color), and an Apple iPhone (Product) Red cellular phone (red in color), that is, the "Devices."

6. The Devices are currently located at the Hardeeville Police Department, 26 Martin St, Hardeeville, SC 29927.

PROBABLE CAUSE

7. The United States, including ATF, is conducting a criminal investigation of Tyrone Evan Lewis GRAYSON regarding possible violations of 18 U.S.C. § 922(o), 18 U.S.C. § 922(g)(1), 18 U.S.C. § 924(c), 21 U.S.C. § 841(a)(1), 26 U.S.C. § 5861(d), and 26 U.S.C. § 5861(e).

8. On January 20, 2021, I met with Task Force Officer (TFO) Dylan Hightower of the 14th Circuit Solicitor's Office and Lieutenant (Lt.) Randal Risher of the Hampton Police Department. Lt. Risher informed me that GRAYSON is an armed drug trafficker operating in and around Jasper County, SC. Lt. Risher stated that a cooperating source (CS) had been communicating with GRAYSON about purchasing firearms and controlled substances. Lt. Risher also indicated that the CS stated, GRAYSON was in possession of a Glock conversion device.[1] Lt. Risher also showed me a video that was purported to have been recorded by the CS of an individual purported to be GRAYSON shooting a pistol with what appeared to be a Glock conversion device attached. Lt. Risher indicated that GRAYSON utilized two phone numbers and provided me with phone numbers, (843) 384-5984 and (843) 694-4917.

9. At the directions of investigators, the CS arranged for the purchase of the Glock conversion device and an "eight ball" of cocaine from GRAYSON.

10. On January 29, 2021, at the direction and control of investigators, the CS exchanged $1,450.00 in pre-recorded U.S. currency for a Glock conversion device and approximately 4.4 gross grams of cocaine from GRAYSON in Hampton County, SC. Lt. Risher

[1] The ATF Firearms and Ammunition Technology Division (FATD) previously provided guidance stating, "A Glock conversion device – commonly referred to as "Glock switch" or "Glock Auto Sear" – is a part, or combination of parts, designed and intended for use in converting a semiautomatic Glock pistol into a machinegun; therefore, it is a "machinegun."

provided me with a screen shot of a text message exchange between GRAYSON and the CS discussing a price for the Glock conversion device and arranging the transaction.

11. The Glock conversion device was sent to ATF's Firearms Technology Criminal Branch (FTCB) where they determined that the device, in and of itself is a combination of parts designed and intended for use in converting a weapon into a machinegun, therefore the device is a machinegun.

12. The cocaine was sent to the DEA Southeast Laboratory where cocaine was confirmed in the composite.

13. On August 11, 2021, a federal grand jury returned an indictment against GRAYSON for the aforementioned firearm and controlled substance violations and an arrest warrant was issued for GRAYSON.

14. On December 6, 2021, Verizon provided records pursuant to a signed Order indicating that the telephone assigned call number, (843) 384-5984 was determined to be effective April 16, 2021, with Verizon and the listed subscriber was Tyrone Grayson at 5894 Calf Pen Bay Rd, Pineland, SC 29934. Prior to April 16, 2021, the call number was associated with a reseller, "Tracfone" from March 16, 2020 to April 16, 2021.

15. On December 9, 2021, a signed tracking warrant was executed on Verizon to provide location information for the telephone assigned call number (843) 384-5984.

16. On December 14, 2021, utilizing data provided by Verizon, investigators located a Toyota Tundra bearing South Carolina license plate, TEA330 that is registered to GRAYSON with the South Carolina Department of Motor Vehicles. The vehicle was parked in a shopping center near the Bluffton and Hardeeville town line. GRAYSON was observed exiting a business, getting into his vehicle, and driving away. Investigators with the Hardeeville Police Department

and the Jasper County Sheriff's Office conducted a traffic stop on GRAYSON and placed him under arrest based on the federal arrest warrant that had been issued for GRAYSON. Investigators recovered a cellular phone [Apple iPhone (Product) Red] from the ground that GRAYSON had dropped while being arrested and he appeared to be utilizing the device at the time of his arrest.

17. During a search of GRAYSON's vehicle, investigators located two (2) firearms with loaded magazines, a large quantity of suspected Oxycodone pills located in pill bottles and a plastic bag, two (2) additional cellular phones [Motorola Type: N57C9 cellular phone (blue in color), Apple iPhone "S" Model A1688 cellular phone, (silver in color)] and a box of plastic baggies. Investigators searched GRAYSON and located approximately $2,215.00 in his pants pocket.

18. At the beginning of the investigation into GRAYSON in January 2021, I was provided with two (2) phone numbers for GRAYSON, indicating that GRAYSON was likely utilizing multiple phones. GRAYSON utilized a cellular phone to discuss prices, arrange and execute the transaction of a Glock conversion device and cocaine with the CS. When GRAYSON was arrested on December 14, 2021, he was found in the possession of three (3) cellular phones, two (2) firearms, a distribution quantity of suspected Oxycodone pills, a box of plastic baggies and a large quantity of U.S. currency. Based on my knowledge, training, and experience working armed drug trafficking investigations, I know that traffickers will often utilize multiple cellular devices and that they often make phone calls, compose text messages, and take and send pictures to facilitate those transactions. I also know that armed drug traffickers will possess firearms to protect themselves, their controlled substances and their

money. I also know that armed drug traffickers often maintain large quantities of U.S. currency and packaging material for controlled substances.

19. Based on my knowledge, training, and experience, I know that armed drug traffickers utilize stash houses and other locations to hide evidence and to meet suppliers and customers. I know that individuals prohibited from possessing firearms often utilize a straw purchaser to purchase firearms on their behalf from a Federal Firearms Licensee (FFL) and that on occasion, the prohibited person will accompany the straw purchaser to the FFL. The revelation of these locations is valuable to an investigation and can aid in identifying possible co-conspirators.

20. GRAYSON has been in custody since he was arrested on December 14, 2021, and the Devices were seized by the Hardeeville Police Department.

21. I have reviewed a NCIC criminal history for GRAYSON and have determined that he has been convicted in South Carolina of crimes punishable by a term of imprisonment of over one year. Thus, GRAYSON is prohibited from possessing firearms and ammunition for purposes of 18 U.S.C. § 922(g)(1). Per my knowledge, GRAYSON has not received a pardon for his South Carolina convictions.

22. GRAYSON was queried in the National Firearm Registration and Transfer Record (NFRTR) and it was determined that GRAYSON does not have any lawfully registered National Firearms Act (NFA) firearms. Thus, GRAYSON is prohibited from possessing and transferring a machinegun for purposes of 18 U.S.C. § 922(o), 26 U.S.C. § 5861(d) and 26 U.S.C. § 5861(e).

23. SA Bryce Eikenberg reviewed the firearms and a sample of the ammunition recovered from GRAYSON's vehicle and determined that they were not manufactured in the state of South Carolina, and therefor traveled in interstate and/or foreign commerce.

24. As a case agent, I have been the affiant on previous electronic search warrants and I have experience and have consulted with others in the fundamentals of mobile communications, electronic and cellular data analysis.

25. In my training and experience, I know that the Devices have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Hardeeville Police Department.

TECHNICAL TERMS

26. Based on my training and experience and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets,

smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling

voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit

boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their

customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

i. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

27. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this

investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including armed drug trafficking utilize cellular phones to facilitate the commission of these criminal acts. Further, I am aware that incriminating evidence is often located within text messages, as well as photos and videos contained on cell phones. Additionally, call logs (for incoming, outgoing, and missed calls), stored contact lists, and location information have proven to be valuable evidence in criminal cases. Moreover, I am familiar with technology, such as Cellebrite mobile data transfer equipment, that allows law enforcement investigators to harvest data (such as incoming and outgoing text messages, photos, videos, call logs, and contacts) from cell phones. I also know that it is common for individuals involved in criminal activity to use cellular phones subscribed in a name other than their own, and to use "pre-paid" cellular phones for which no real subscriber information is available. In addition, based on my experience, I know that individuals in possession of firearms and engaged in armed drug trafficking often utilize mobile telephones and other electronic devices to communicate with customers, receive orders, make purchases, create ledgers and to arrange for dissemination of controlled substances and firearms. Often times, photographs are taken of firearms and controlled substances to facilitate transactions. These photographs can be maintained on cellular telephones.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

29. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did

not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This

data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose

of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

30. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic

files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend

themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or

assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

31. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

32. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a warrant to search the Devices described in Attachment A and to seize the items described in Attachment B.

This affidavit has been reviewed by SAUSA Carra Henderson.

Respectfully submitted,

ROBERT CALLAHAN Digitally signed by ROBERT CALLAHAN
Date: 2022.02.02 10:41:29 -05'00'

Robert Callahan
Special Agent
Bureau of Alcohol, Tobacco, Firearms & Explosives

Subscribed and sworn to before me
on February 2, 2022

HON. MARY GORDON BAKER
UNITED STATES MAGISTRATE JUDGE